HPE StoreEver MSL3040/6480 Tape Library

KeyControl® Integration Guide

2024-07-10

Table of Contents

Chapter 1. Introduction

This document describes the integration of the Hewlett Packard Enterprise (HPE) StoreEver MSL3040/6480 Tape Library (referred to as StoreEver in this guide) with the Entrust KeyControl key management solution using the open standard KMIP protocol. KeyControl serves as a key manager for encryption keys by using various protocols, including KMIP.

1.1. Product configurations

Entrust has successfully tested the integration of KeyControl with HPE StoreEver MSL3040/6480 Tape Library in the following configurations:

System	Version
Entrust KeyControl	10.2

1.2. Requirements

Before starting the integration process, familiarize yourself with:

- HPE StoreEver MSL3040 Tape Library User and Service Guide
- HPE StoreEver MSL6480 Tape Library User and Service Guide
- Entrust KeyControl Online Documentation Set

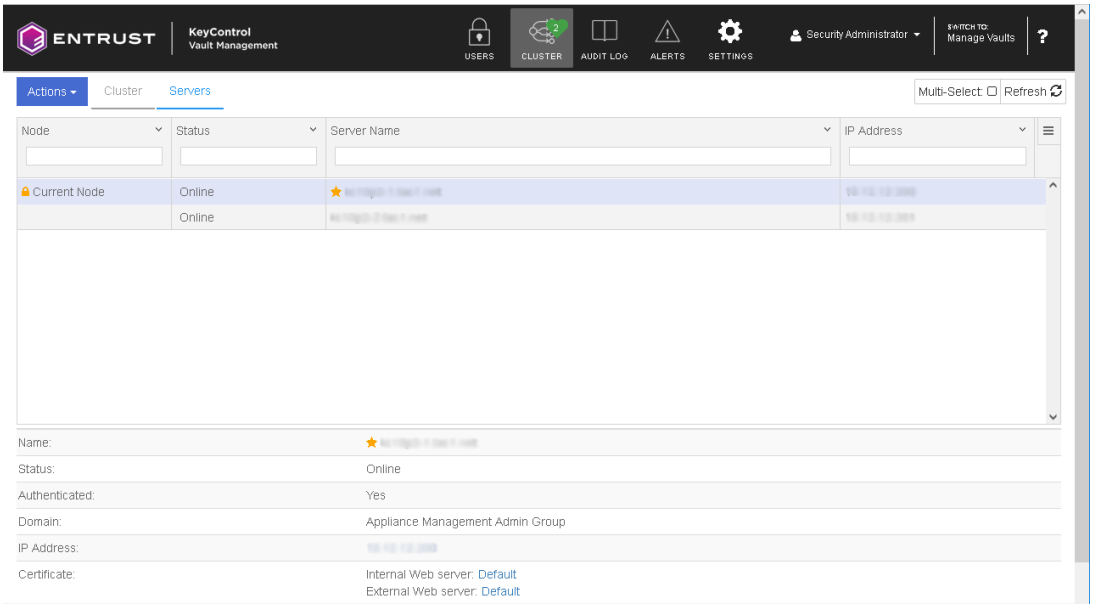
Chapter 2. Deploy and configure KeyControl

2.1. Deploy a KeyControl cluster

For the purpose of this integration, a two-node cluster was deployed as follows:

1. Download the KeyControl software from Entrust TrustedCare. This software is available as an OVA or ISO image. This guide deploys an OVA installation.
2. Install KeyControl as described in KeyControl OVA Installation.
3. Configure the first KeyControl node as described in Configuring the First KeyControl Node (OVA Install).
4. Add second KeyControl node to cluster as described in Adding a New KeyControl Node to an Existing Cluster (OVA Install).

Both nodes need access to an NTP server, otherwise the above operation will fail. Sign in to the console to change the default NTP server if required.



5. Install the KeyControl license as described in Managing the KeyControl License.

2.2. Additional KeyControl cluster configuration

After the KeyControl cluster is deployed, additional system configuration can be done as described in KeyControl System Configuration.

2.3. Configure authentication

This guide uses local account authentication.

For AD-managed Security groups, configure the LDAP/AD Authentication Server as described in Specifying an LDAP/AD Authentication Server.

2.4. Create DNS record for the KeyControl cluster

This guide uses the individual IP addresses of the KeyControl nodes.

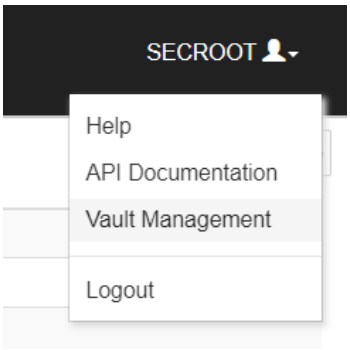
To use hostnames, configure your DNS server giving each node in the KeyControl a unique name.

2.5. Create a KMIP Vault in the KeyControl

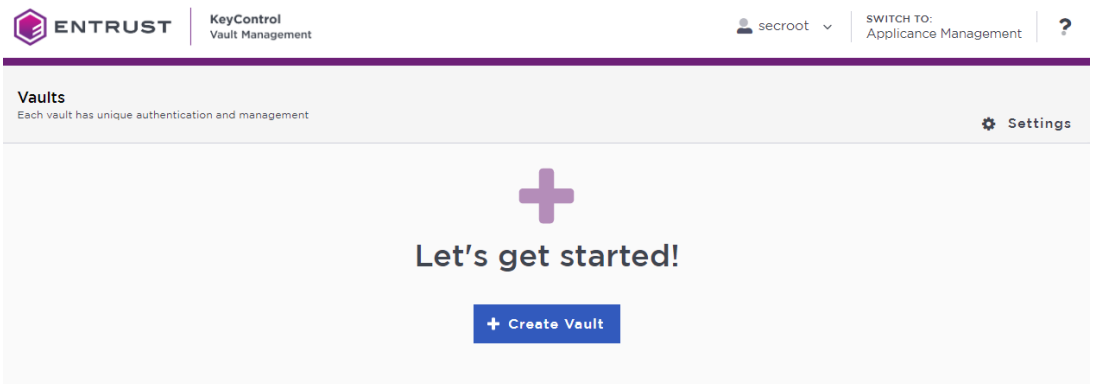
The KeyControl Vault appliance supports different type of vaults. For example: cloud key management, KMIP, PASM, database, and others. This section describes how to create a KMIP vault for tis integration.

Refer to the Creating a Vault section of the admin guide for more details.

1. Sign in to the KeyControl Vault Server web user interface:
    a. Use your browser to access the IP address of the server.
    b. Sign in using the **secroot** credentials.
2. From the user's dropdown menu, select **Vault Management**.

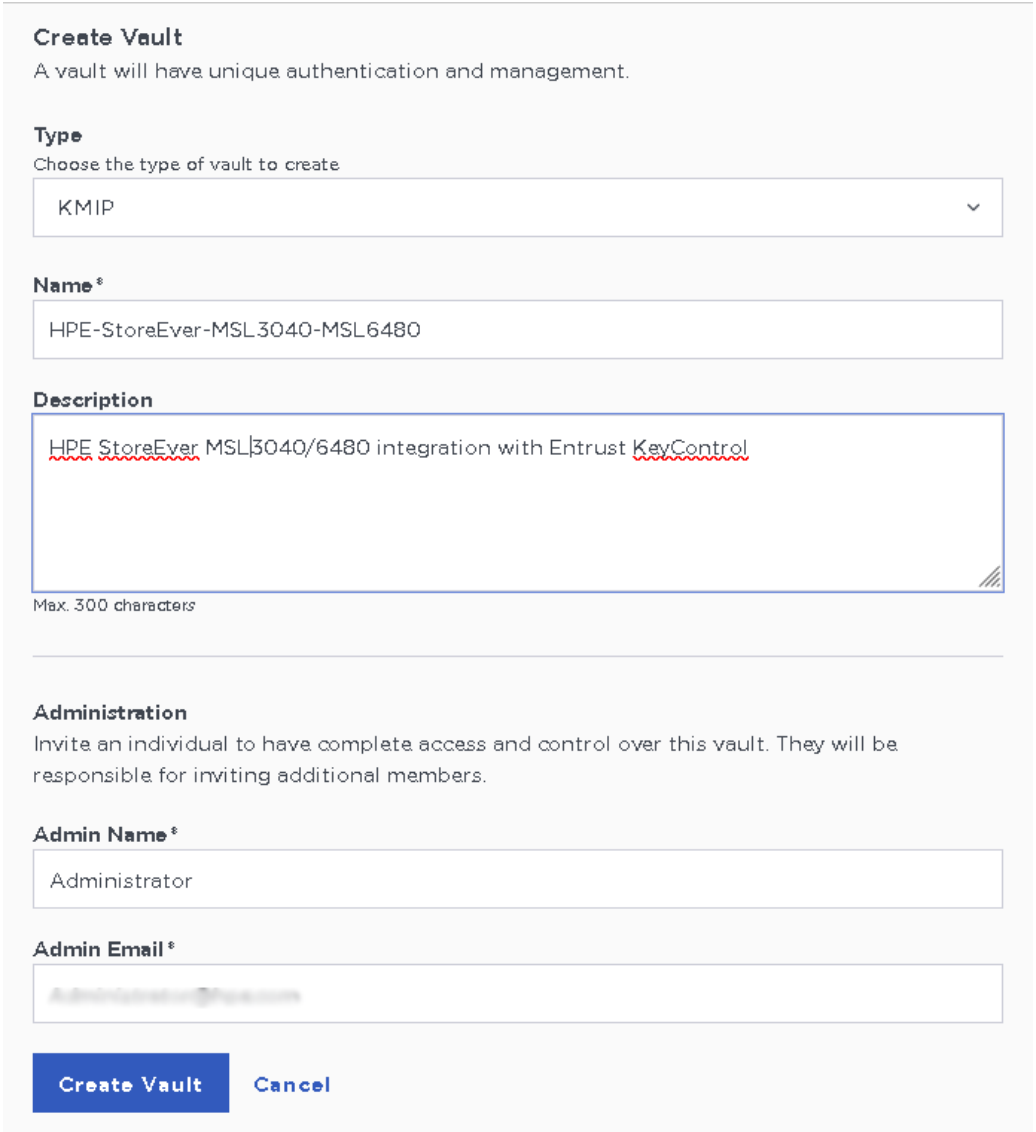


3. In the KeyControl Vault Management interface, select **Create Vault**.



4. In the **Create Vault** page, select **KMIP**. Then enter your information.

   For example:

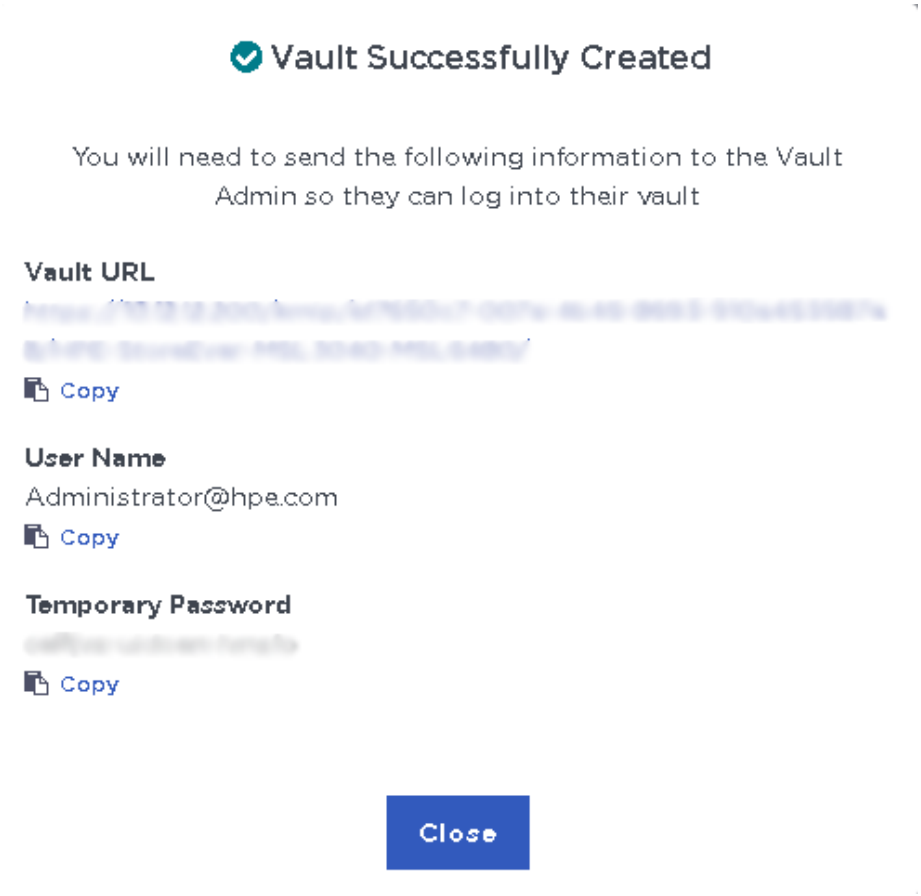


5. Select **Create Vault**, then select **Close**.

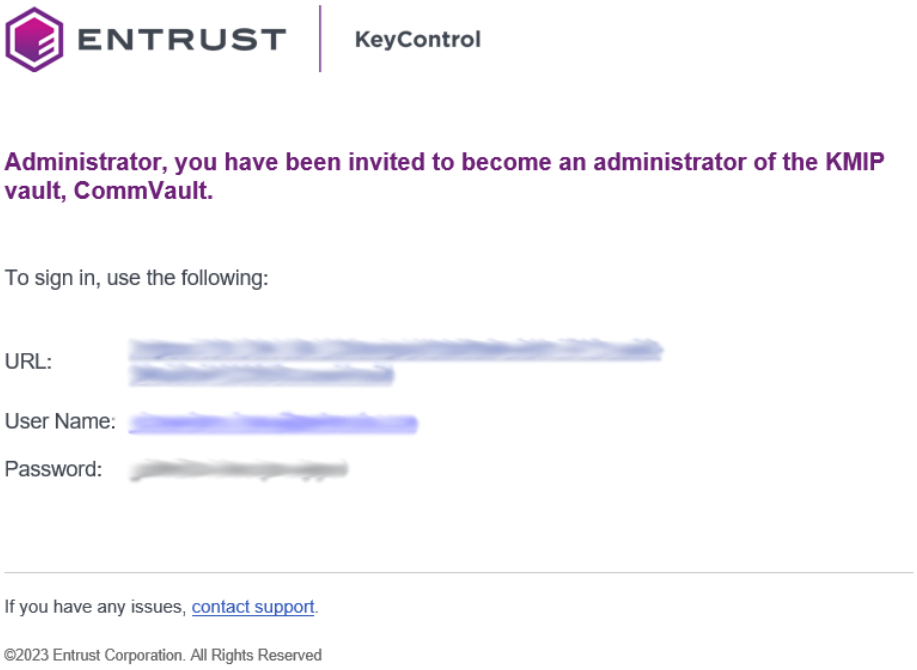
   A window with the newly created vault information appears. In addition, an email with

the same vault information is sent to the security administrator **secroot**.

Example vault information window:



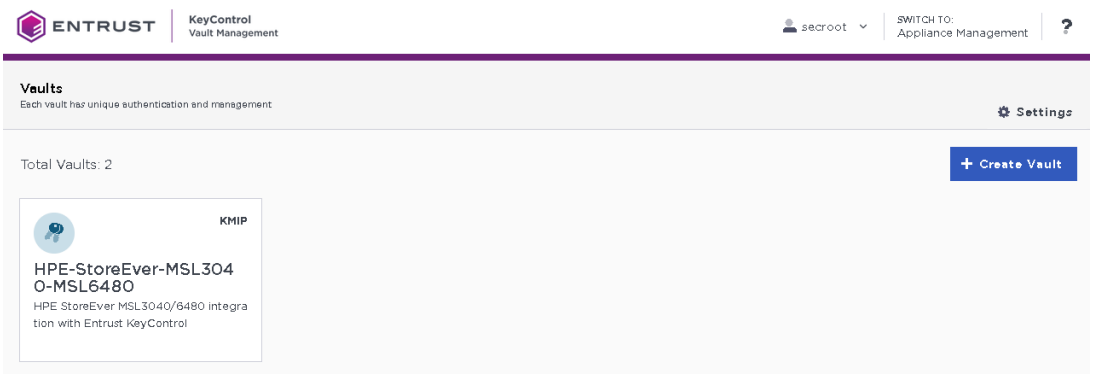
Example email:



6. Bookmark the **Vault URL** listed above.

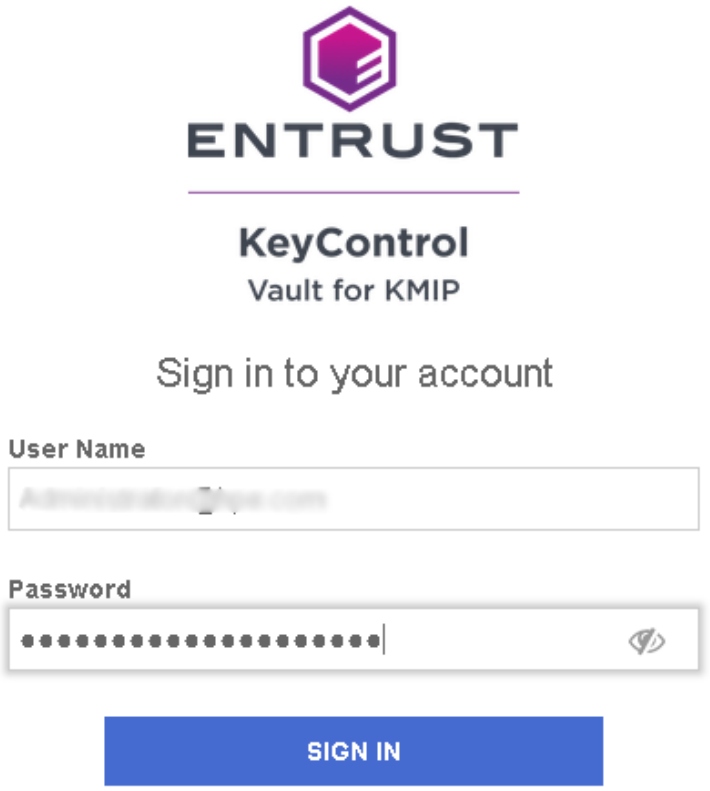
   The newly created Vault is added to the **Vault Management** dashboard.

   For example:



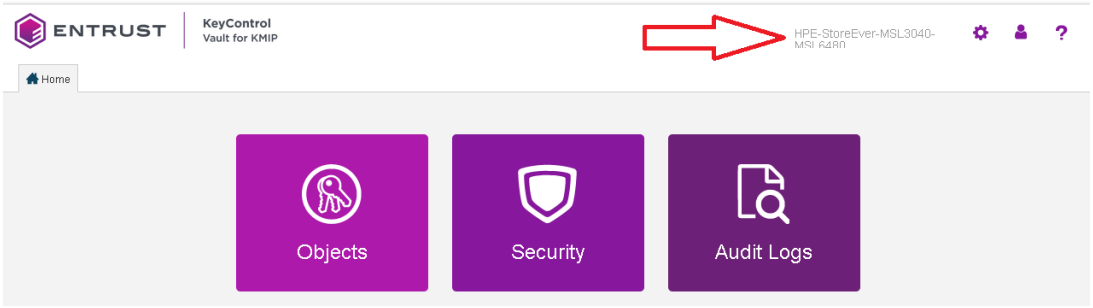
7. Sign in to the **Vault URL** with the temporary password. Change the initial password when prompted. Sign in again to verify.

   For example:



8. Notice the new vault.

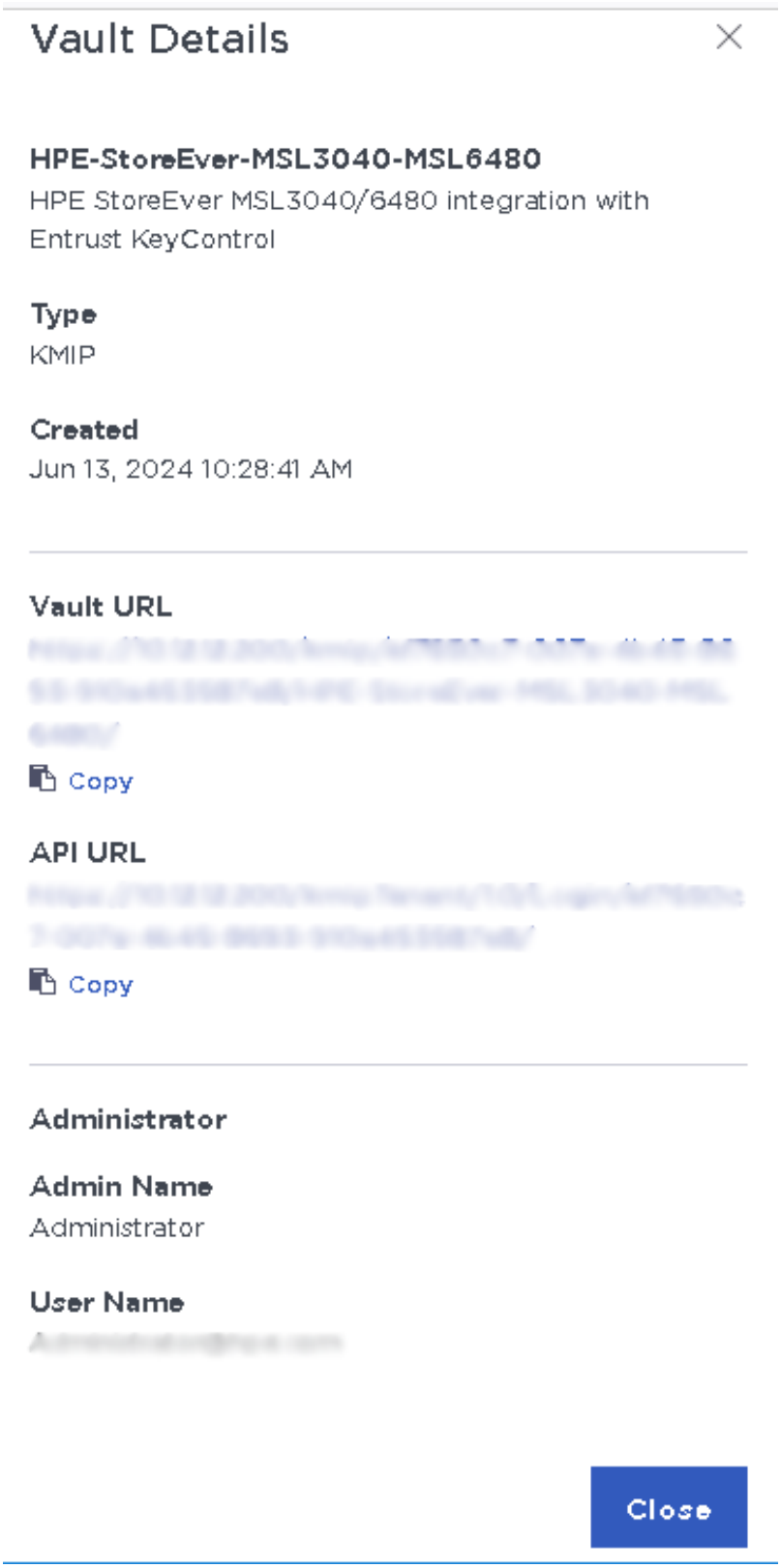
   For example:



2.6. View the KMIP Vault details

1. Hover over the Vault and select **View Details**.

   For example:



2. Select **Close** when done.

Chapter 3. Integrate KeyControl with StoreEver

Follow these steps to register Entrust KeyControl as a KMS in HPE StoreEver Tape Library.

1. Obtain the CA certificate
2. Configure the KMIP server
3. Create the client certificate bundle
4. Import tenant client certificate into the StoreEver Tape Library
5. Set the default encryption mode

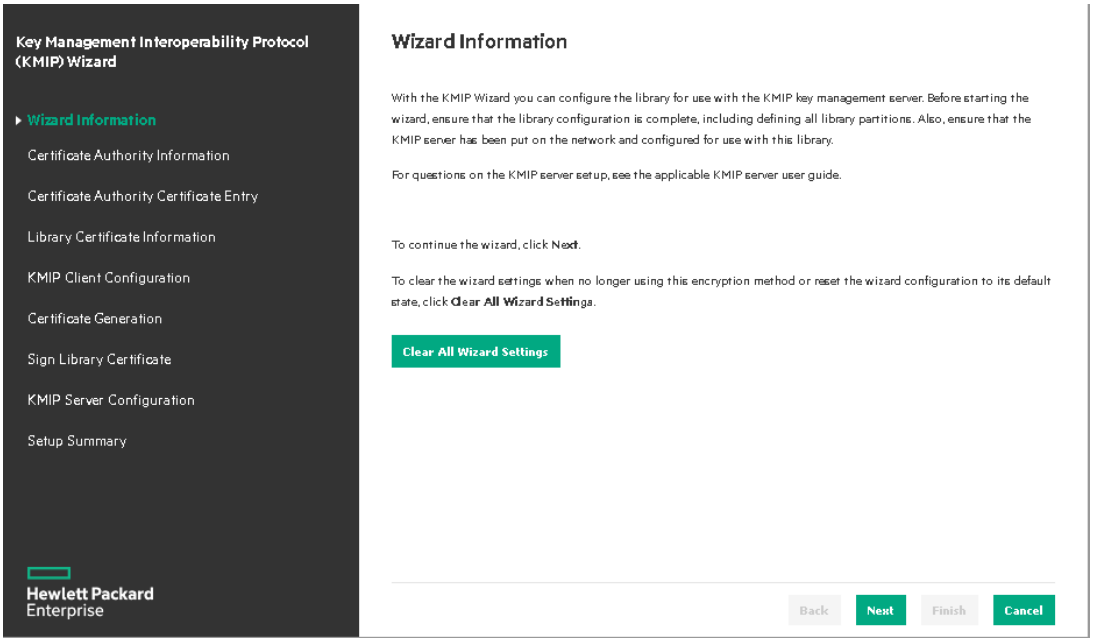
3.1. Obtain the CA certificate

The Entrust KeyControl KMIP server can accept a certificate from your local root CA or a trusted CA, or can act as local root CA itself. For the purpose of this integration the Entrust KeyControl KMIP server will act as the local root CA. Execute the following steps to obtain the local root CA certificate for the Entrust KeyControl KMIP server.

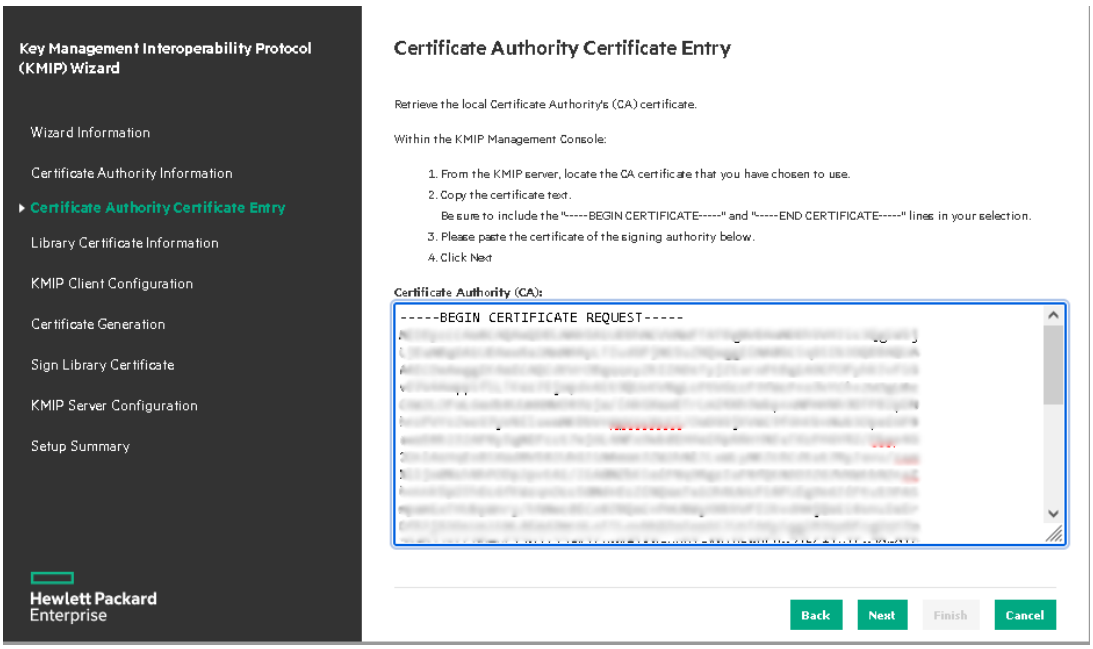
1. Sign in to the KMIP Vault with the URL and credentials from Create a KMIP Vault in the Entrust KeyControl.
2. Go to the **Vault Management** window by selecting **SWITCH TO Manage Vaults / SWITCH TO Appliance Management** in the top right corner of the window.
3. Select the **?** icon in the top right corner of the window, then select **Download CA certificate**.
4. Save the certificate for later use. Example filename: `240614140352_cacert.pem`.

3.2. Configure the KMIP server

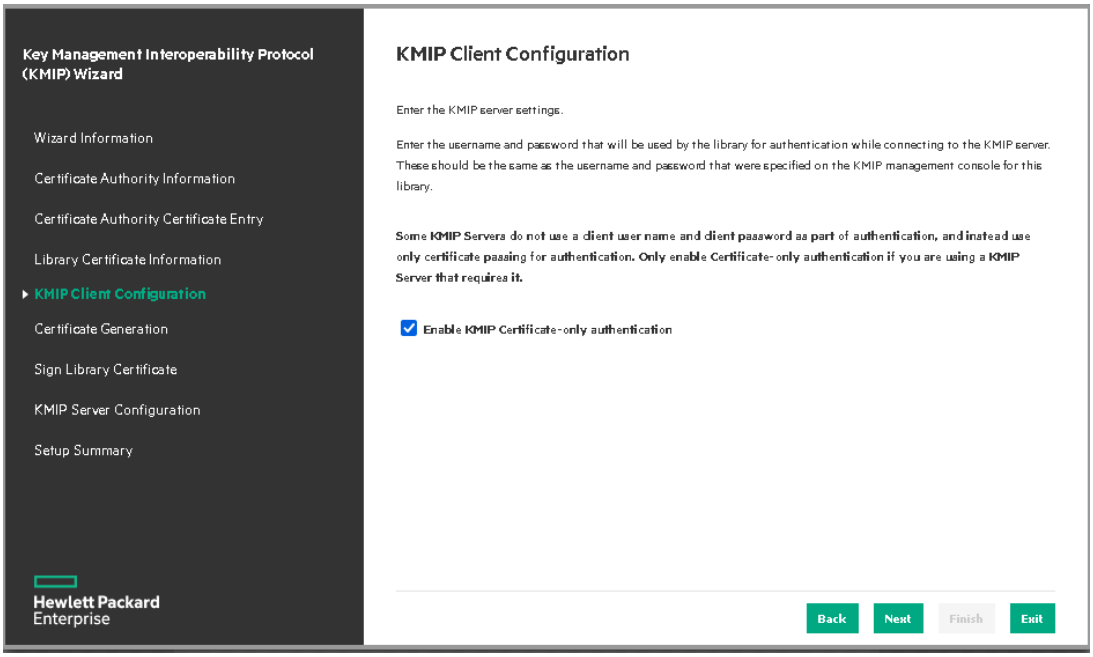
1. Log into the StoreEver webGUI using an account with Security Admin privileges.
2. Select the **Configuration** box.
3. Expand the **Encryption** menu in the right toolbar, then select **KMIP Wizard**.



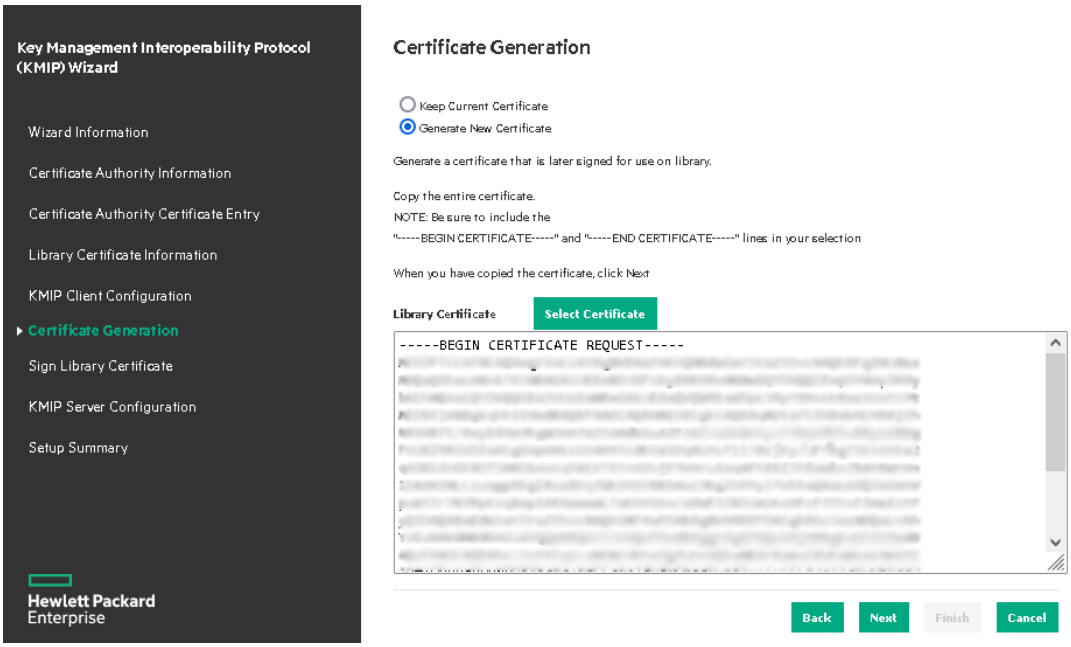
4. Select **Clear All Wizard Settings** to remove any prior configuration.
5. Select **Next** twice.
6. In the **Certificate Authority Certificate Entry** window, copy-paste the certificate from section Obtain the CA certificate into the **Certificate Authority (CA):** text box, then select **Next**.



7. Select **Next** twice.
8. In the **KMIP Client Configuration Window**, check **Enable KMIP Certificate-only authentication**, then select **Next**.



9. In the **Certificate Generation** window, select the **Generate New Certificate** radio button.
10. When certificate request has been generated, copy the certificate request to a file, for example, `hpe-storeever-3040.csr`, then select **Next**.



11. Pause configuring the KMIP server. You will continue further down.

3.3. Create the client certificate bundle

1. Sign in to the KMIP Vault with the URL and credentials from section Create a KMIP

Vault in the Entrust KeyControl.

2. Select **Security**, then **Client Certificates**.

3. In the **Manage Client Certificate** page, select the **+** icon on the right to create a new certificate. The **Create Client Certificate** dialog box appears.
4. In the **Create Client Certificate** dialog box:

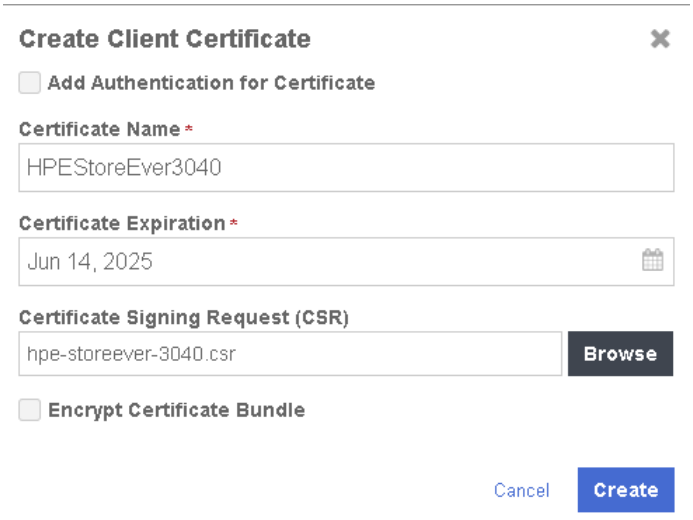
   a. Enter the **Certificate Name**.

   b. Select the **Certificate Expiration**.

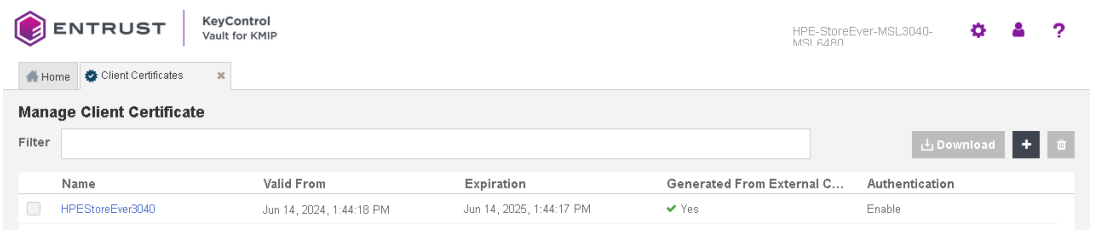
   c. Upload the certificate request created in section Configure the KMIP server.

   d. Select **Create**.

   For example:



   The new certificates are added to the **Manage Client Certificate** pane.



5. Select the certificate and select the **Download** icon to download the certificate.

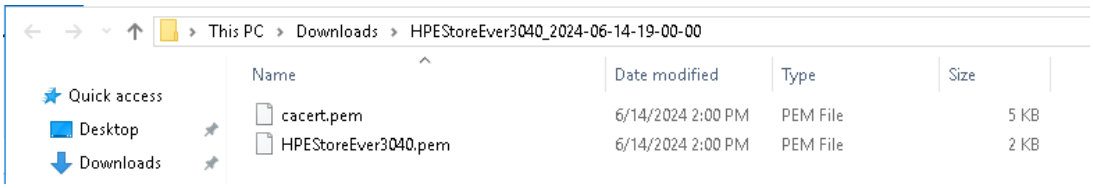
6. Unzip the downloaded file. It contains the following:

   - A `certname.pem` file that includes both the client certificate and private key. In this example, this file is called `HPEStoreEver3040.pem`.

     The client certificate section of the `certname.pem` file includes the lines **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** and all text between them.

     The private key section of the `certname.pem` file includes the lines **-----BEGIN PRIVATE KEY-----** and **-----END PRIVATE KEY-----** and all text in between them.

   - A `cacert.pem` file which is the root certificate for the KMS cluster. It is always named `cacert.pem`.



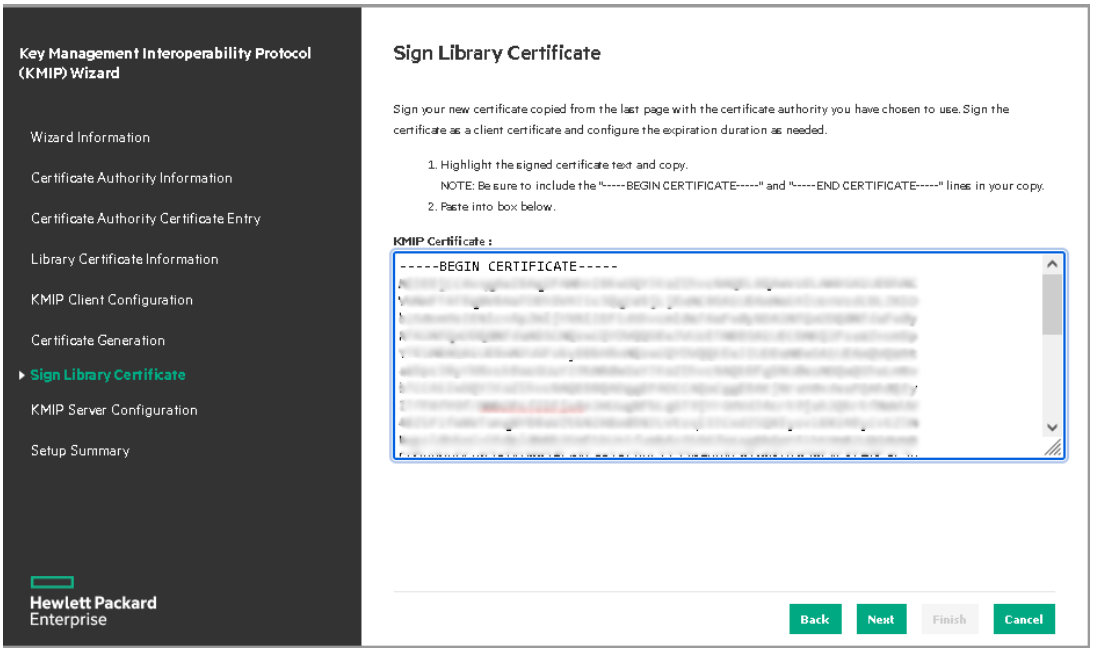
See the following link for additional information Managing KMIP Objects in the KeyControl KMIP Vault webGUI.

3.4. Import tenant client certificate into the StoreEver Tape Library

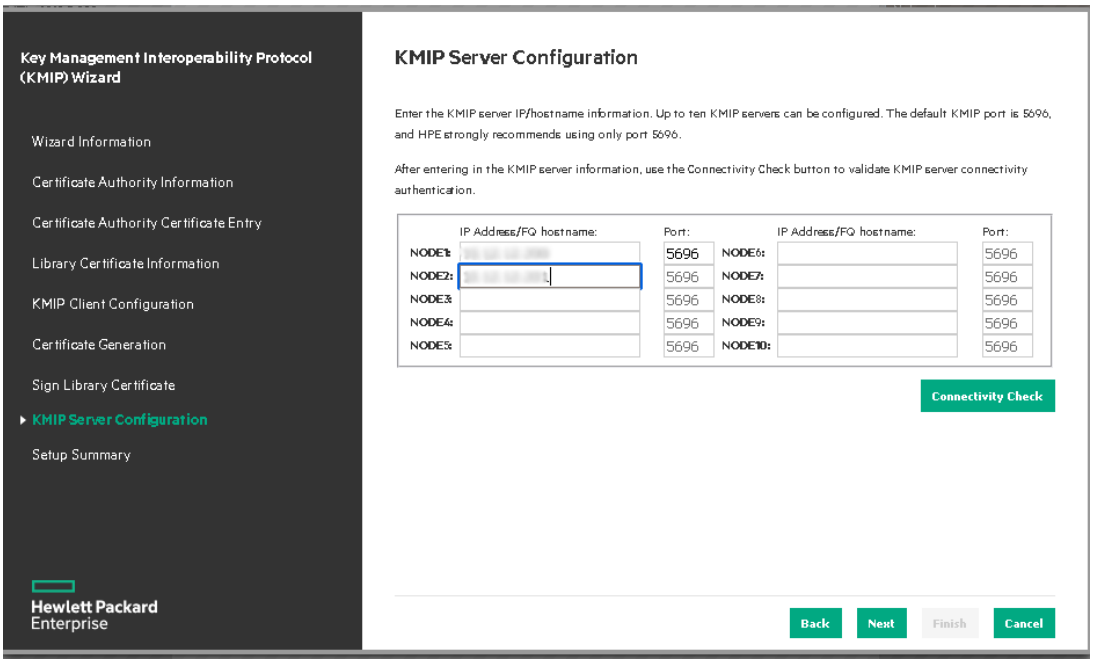
This resumes section Configure the KMIP server.

1. In the **Certificate Generation** window, select the **Keep Current Certificate** radio button this time.
2. In the **Signed Library Certificate**, paste the certificate created in section Create the client certificate bundle, then select **Next**.

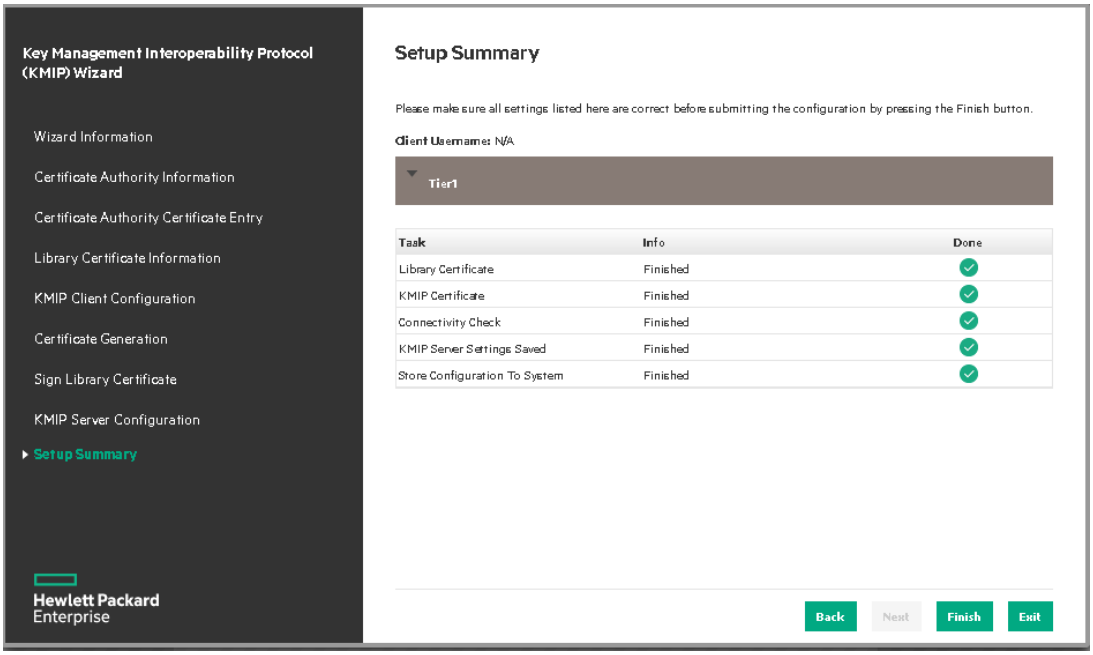
   File `HPEStoreEver3040.pem` contains the certificate.



3. In the **KMIP Server Configuration** window, enter the IP of the Entrust KeyControl KMIP server nodes. Select **Connectivity Check** to test connectivity to the nodes, it should check OK, then select **Next**

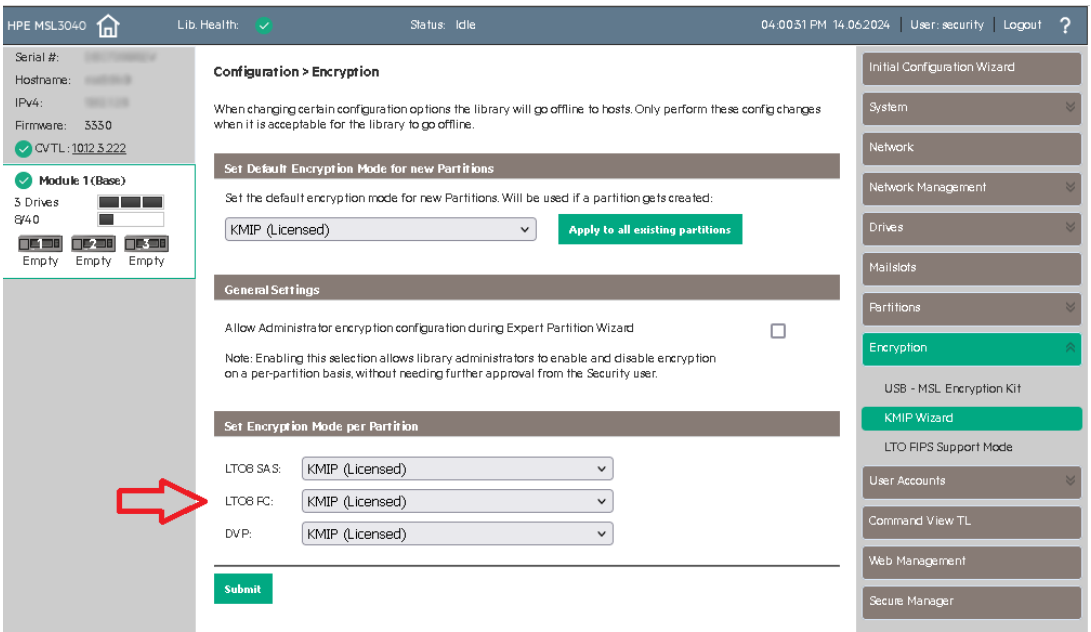


4. In the **Setup Summary** windows, select **Finish**, then select **Exit**.



3.5. Set the default encryption mode

1. Log into the StoreEver webGUI using an account with Security Admin privileges.
2. In the **Set Default Encryption for new Partitions** section, select **KMIP (Licensed)** from the pull-down menu.
3. Select **Apply to all existing partitions**. Notice the change in **Set Encryption Mode per Partitions**.



4. Select **Submit**.

Chapter 4. Test the integration

Testing is done using the HPE Library and Tape Tools (L&TT). Within this tool, the Drive Performance test writes and reads data to/from the specified tape drive. The Entrust KeyControl KMIP server manages the keys for the writes and reads operations. Therefore, the entire system is tested.

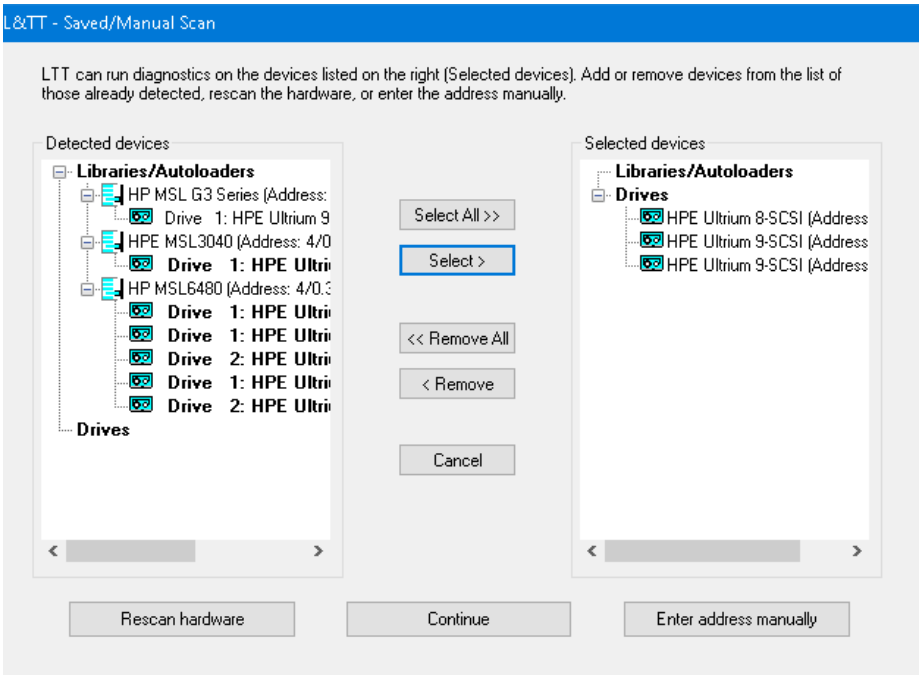
This test needs a tape manually loaded in the drive(s).

This test will overwrite all data on the tape, meaning that the data will be lost.

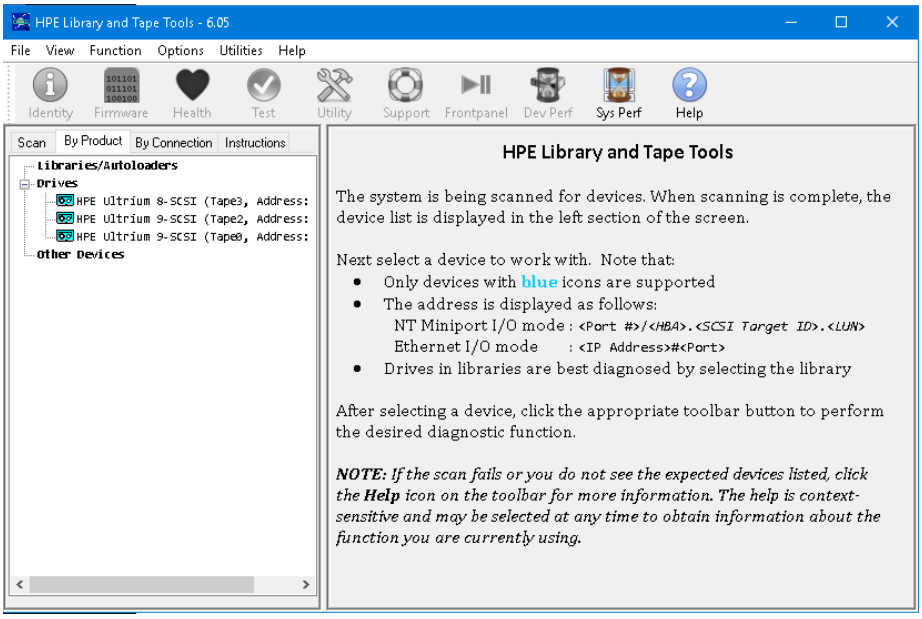
1. Launch the **HPE Library and Tape Tools**.
2. In **L&TT - Startup**, select **Saved/Manual Scan**, **NT Miniport**, **Check for Backup Applications and Services**, then select **Continue**.

3. All devices available for testing should appear in the **Detected devices** left pane.

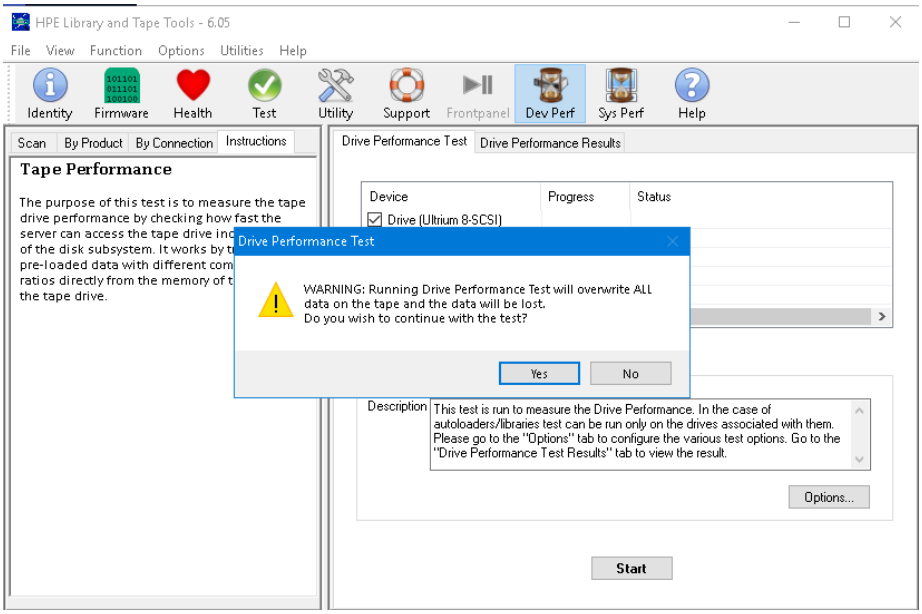
4. Expand the device(s) to test in the **Detected devices** pane.
5. Select a **Drive** of a device to test, not the actual device itself. Then select **Select**. Repeat until all the drives to test appear in the **Select devices** pane. Then select **Continue**.



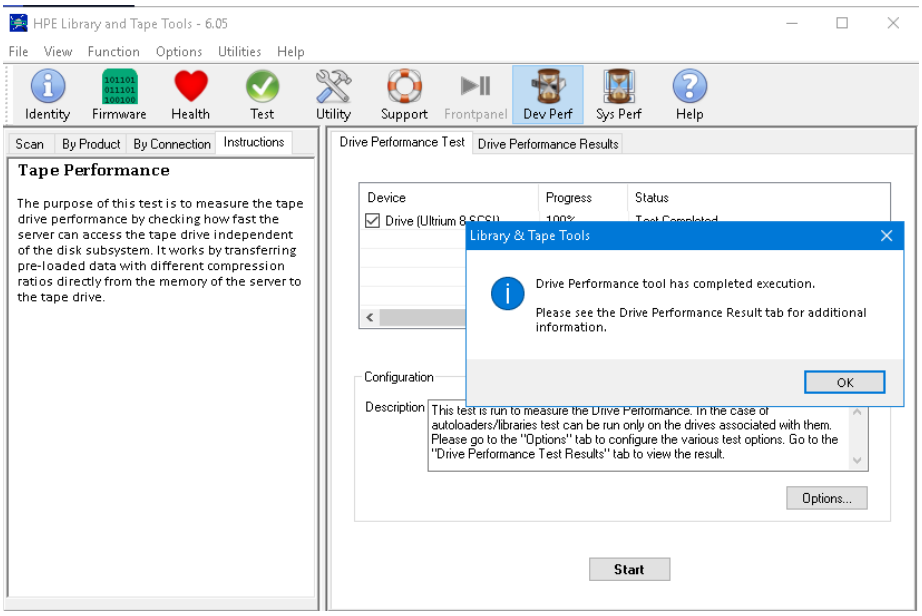
6. Wait for the scan to complete. The **By Product** tab in the left pane displays the selected drive(s).



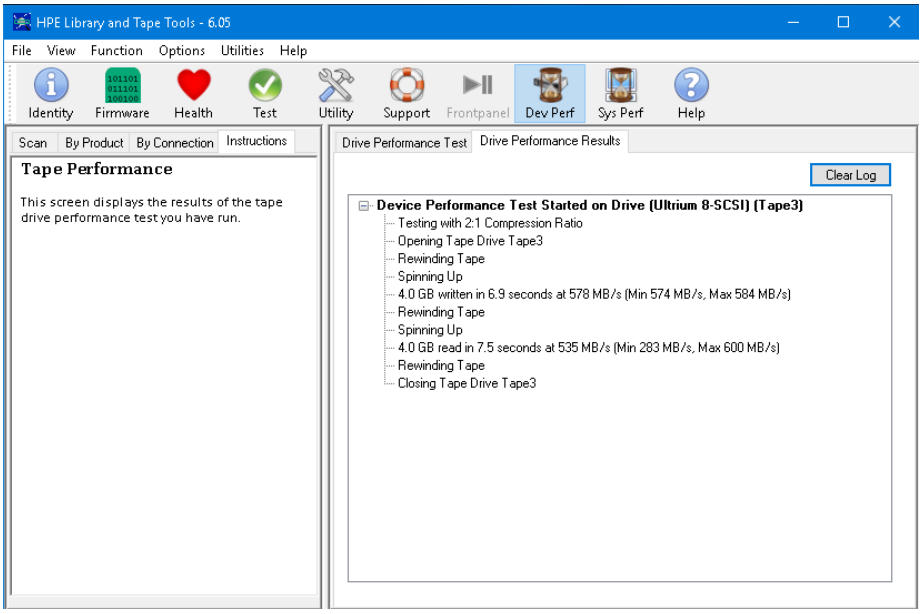
7. Select a drive. Then select **DevPerf** in the toolbar. Then select **Start**.



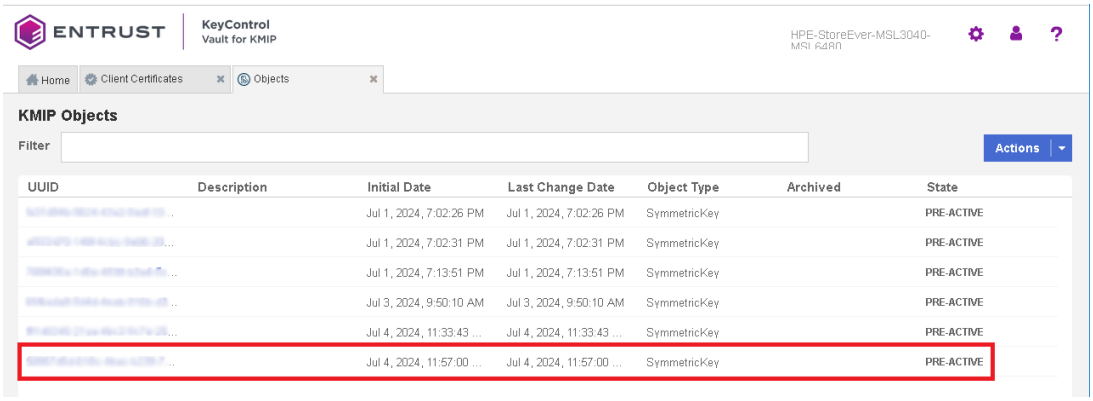
8. Acknowledge the warning. Then wait for the test to complete. Then select **OK**.



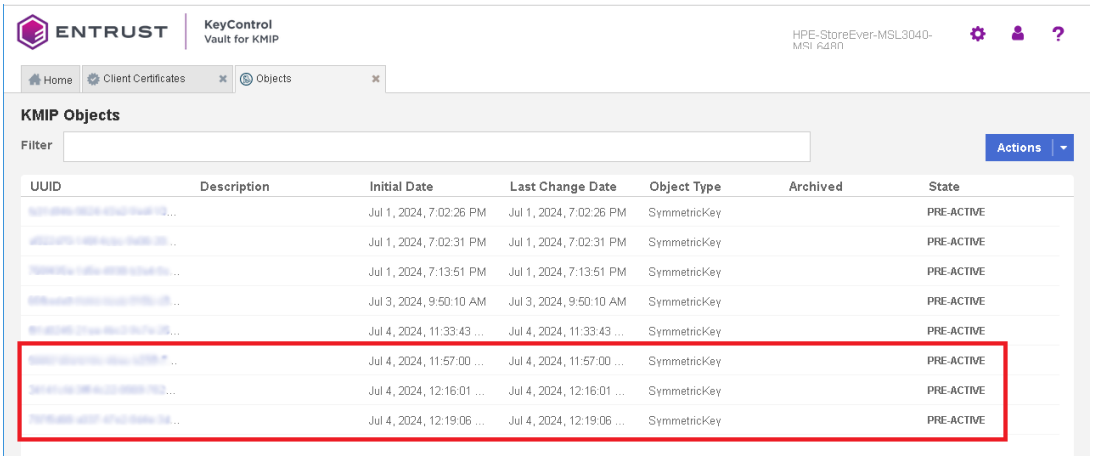
9. Select the **Drive Performance Results** tab to view the results.



10. Sign in to the KMIP Vault with the URL and credentials from Create a KMIP Vault in the Entrust KeyControl.
11. Select the **Objects** tab. Notice the symmetric key created during the testing conducted above.



12. Back in the **HPE Library and Tape Tools** window, select the **By Product** tab in the left pane.
13. Repeat steps for additional drives.



Notice the three symmetric keys created to test the three drives above.

Chapter 5. Integrating with an HSM

For guidance on integrating the Entrust KeyControl with a Hardware Security Module (HSM), consult with your HSM vendor. If you are using an Entrust nShield HSM, refer to the Entrust KeyControl nShield HSM Integration Guide available at Entrust documentation library.

Chapter 6. Additional resources and related products

6.1. Entrust products

6.2. nShield product documentation